

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

Filed Under Seal Pursuant to Local Rule 157.6(a)

I, Michel J. Verhar, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and I have been employed as a Special Agent with the FBI since 2001. I am currently assigned to the Bangor, Maine Resident Agency. I am a law enforcement officer of the United States empowered by law to conduct investigations of and to make arrests for federal offenses, including that contained in Title 18, United States Code, Section 876.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at **110 Twin Hills Road, Burlington, Maine**, as more particularly described in Attachment A to this affidavit (hereinafter the "Target Premises"), and to seize the items described in Attachment B to this affidavit.

3. This affidavit is intended to provide the facts necessary for a determination of probable cause. Based on my training and experience, there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. § 876 (mailing threatening communications) are presently located at the Target Premises. I am requesting authority to search the entire Target Premises, including the residential dwelling, and any garage, shed, outbuilding or storage unit assigned to that dwelling, for the items specified in Attachment B hereto, which items constitute instrumentalities and evidence of the foregoing violation.

4. The statements contained in this affidavit are based upon my investigation, information provided by other sworn law enforcement officers, and on my experience and training as a federal agent.

PROBABLE CAUSE

Mailing One

5. On October 15, 2018, multiple law enforcement agencies responded to the residence of Thomas Daffron and his spouse U.S. Senator Susan Collins, located in Bangor, Maine, after being notified by Daffron that he had opened and handled a letter purportedly contaminated by ricin. In summary, Daffron informed investigators that he was opening mail while at the house alone. He opened an envelope that was addressed to him and began reading the enclosed letter. The typed and unsigned letter claimed to have been “coated in Ricin residue”, said “Good Luck to you and Susan in the next life” and stated “your wife has betrayed the people of Maine along with the American people and this will be her downfall.” The envelope bore a Bangor, Maine return address and a name but was postmarked in both Tacoma and Olympia, Washington on October 12, 2018.

6. Two hazardous materials response teams responded to the residence, and conducted preliminary field tests for the presence of biological toxins before determining that no hazardous materials were present. Daffron was then interviewed. The FBI and U.S. Postal Inspection Service (USPIS) participated in the transport of the threatening letter to the Health and Environmental Testing Laboratory (HETL) in Augusta and in the interview of Daffron.

7. I subsequently conducted an interview of the person identified in the return address on the envelope of Mailing One. The person, a male, denied involvement in sending the letter described in paragraph 5 above.

Mailing Two

8. As a result of Mailing One, USPIS supervisors assigned a U.S. Postal Inspector to hand-screen all mail addressed to the Daffron and Collins residence. On October 17, 2018,

inside the USPS mail sorting facility in Hampden, Maine, the Postal Inspector examined a hand-printed envelope that was addressed to "Susan Collins or current resident", bore her street address, and a return street address corresponding to a residence in Bangor, Maine (different from the Bangor return address on Mailing One). The Postal Inspector observed a fine white powder leaking from the envelope. He initiated his standard operating procedures for handling and field testing potentially hazardous mail, and determined that no hazardous materials were present. The Inspector and I spoke and he then transported the letter to the HETL in Augusta.

9. While the envelope and the contents were being tested at the HETL, the Postal Inspector and I interviewed the owner of the home located at the return address on Mailing Two. That home happens to be where Collins and Daffron lived immediately prior to moving to their current home. The current owner stated that he and his wife purchased the house in 2013, which is consistent with database and records searches that I conducted prior to the interview. He and his wife became aware that Collins and Daffron were the previous owners when they received mail at their home addressed to Daffron and Collins. The current owner denied he had ever searched for Collins' new home address or that had he ever mailed anything to either Daffron or Collins.

10. After conducting multiple tests, the HETL advised me that the envelope, powder, and contents of the envelope were negative for ricin toxin as well as negative for several other toxic substances.

11. The HETL provided me photographs of the envelope and the contents. Inside the envelope was a double-sided, Aetna Medicare Solutions colored flyer. On one side of the flyer there is blue handwriting. The handwriting reads, "AnthRAX!!! HA HA HA!!!" A stick-figure

face has been drawn with the letter "X" for eyes, the tongue sticking out, and with "You" and an arrow pointing at the stick figure face.

12. After accepting custody of the envelope and the contents comprising Mailing Two from the HETL, I entered the items into FBI evidence and had them transferred to the FBI Laboratory in Quantico, Virginia, and requested forensic examinations.

13. The FBI Chemistry Unit advised the fine white powder inside the envelope was consistent with starch. The chemist who conducted the examination advised the Unit would not conduct a comparison with similar materials due to starch being a common household substance.

14. The FBI Questioned Documents Unit (QDU) advised me that the writing on the envelope and flyer comprising Mailing Two is suitable for handwriting comparison, and dictated and undictated known writing should be obtained from a suspect for the comparison. The writing instrument on the Aetna flyer was a blue crayon. The envelope bears two self-adhesive, 2014 Star Spangled Banner U.S. Postage stamps. The stamps have a black background and have multi-colored fireworks in the middle. Lastly, the QDU advised that the edges on the Aetna flyer have been cut and are suitable for comparison with similar paper fragments that have been cut.

15. The FBI Latent Fingerprint Unit identified one friction ridge print on the exterior of the envelope. The print was a match in the Next Generation Identification (NGI) system for the right thumb print of Suzanne Elizabeth Muscara, date of birth in January 1982. NGI is the FBI's friction ridge print database. That database collects fingerprints received from state and federal law enforcement agencies. Muscara was arrested in Pennsylvania in 2013 and her fingerprints were collected in connection with that arrest.

Additional Facts

16. I searched Maine State databases and learned Suzanne Muscara has a Maine driver's license, which lists a home address of P.O. Box 113, Burlington, Maine. Burlington is located approximately 50 miles northeast of Bangor. A commercial database showed Muscara as associated with the addresses 33 Sibley Road and 110 Twin Hills Road, both in Burlington. I conducted a search of NCIC queries on Muscara. That led me to contact a park ranger in Alabama who told me that on January 12, 2019, he found Muscara sleeping in her car in Gulf Shores State Park in Alabama. He told me it appeared she was living in her car, a blue Honda with Maine plates, due to the quantity of food, blankets and other belongings he observed. I also spoke with a police dispatcher in Mississippi, who advised that her department had received a call to check on a motorist on February 11, 2019. Muscara was the occupant of the vehicle, a blue Honda registered in Maine. My search also showed that Muscara was queried by the Knoxville, Tennessee, Police Department on March 10, 2019.

17. I interviewed a cooperating witness (CW-1), a resident of Burlington, Maine, in February of this year. CW-1 told me that she met Muscara several years ago. CW-1 advised that she had advertised land for sale on the Internet, and Muscara contacted her about the land. Muscara bought the property located at 33 Sibley Road from CW-1 in December 2013. Muscara lived in a trailer that CW-1 had left on the property. In late 2017, there was a fire and the trailer was destroyed and Muscara was injured. After the fire, Muscara told CW-1 that she was going to stay with relatives in New Jersey while she was recovering from her injuries. When Muscara returned to Burlington, CW-1 rented her a cabin to live in. CW-1 told me that she has not seen any visitors or others at the cabin since Muscara moved in. The address of the cabin is 110 Twin Hills Road, Burlington, Maine. Muscara moved to the cabin in either in April or May, 2018, and

paid CW-1 \$300 a month for rent. CW-1 told me that Muscara left for New Jersey in December, 2018 or January, 2019. Muscara told CW-1 she would be back in April to collect her things. CW-1 is not charging rent during Muscara's absence. When I first spoke with CW-1 in February, 2019, she had not spoken to Muscara since early January, 2019.

18. When I met with CW-1 again on March 27, 2019, she said Muscara showed up without notice about four weeks ago. Muscara told CW-1 she wanted to check on her belongings. Muscara said she would be back in April to remove her property, as she was planning on moving in with family in New Jersey. CW-1 did not see Muscara remove anything from the cabin during the few hours Muscara was there. I spoke with CW-1 on April 2, 2019, and she told me that she does not believe that Muscara has returned yet to gather her belongings from the cabin.

19. When I spoke with CW-1 in February, she told me that Muscara used a computer to watch "tapes" at the cabin that Muscara rented from CW-1. She said that Muscara did not have internet service at the cabin. According to CW-1, Muscara would drive to a library in Burlington when she wanted to access the internet on her phone. CW-1 provided me with a cell phone number and email address that Muscara had used in communicating with her. When I spoke to CW-1 again on March 27, she clarified that Muscara watched movies on a tablet. She said that Muscara would drive to Burlington or to Lincoln, Maine in order to use the internet.

20. I spoke with the Maine Department of Labor on January 25, 2019, and determined it had no information indicating that Suzanne Muscara earned any wages in Maine. I believe that if Muscara had been employed at any time by the United States Postal Service that such wages would have been reported to the Maine Department of Labor. Therefore, her thumbprint on the

exterior of the envelope as noted above cannot be explained by her handling that envelope as an employee of the Postal Service.

21. I have learned of no connection between Muscara and the male whose name was included with the return address on Mailing One.

22. I spoke again with CW-1 on April 2, 2019. She told me that Muscara had spent the previous night in the cabin at 110 Twin Hills Road in Burlington. She said that Muscara had arrived in a small blue car. I have obtained a record from the State of Maine showing that a four-door 2010 Honda Civic, blue in color, is currently registered to Muscara. The license plate number on that vehicle is 3153WH.

23. Based on my involvement with this investigation, I know that the address for Susan Collins that is written on Mailing Two and the return address that is also written on Mailing Two are correct addresses for Susan Collins's current address and her prior address. The connection between Susan Collins and those addresses is not readily available to the public but can be made through internet research.

24. Based on my training and experience, I know that wireless telephones are portable and that people often carry wireless telephones on their person. I also know that wireless telephones have a range of capabilities including storing text messages and e-mail, storing information on personal calendars, and accessing and downloading information from the internet. I also know that computer tablets are portable and that tablet owners and users often carry tablets on their person and in vehicles when they travel. A tablet is a mobile computer and can be used to access the internet through cellular networks, "wi-fi" networks, or otherwise.

25. Based on my training and experience, I know that individuals who threaten public or political figures often seek and collect information about those figures. That information can

include news articles, social media and internet postings and stories, and biographical information about those figures.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Target Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other electronic storage media. Thus, the warrant applied for would authorize the seizure of any computers or other electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

27. I submit that if a computer or storage medium is found on the Target Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not

currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

28. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Target Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of

information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the

computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime

(e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

29. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast

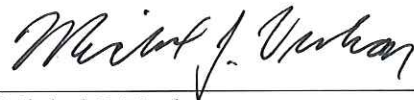
array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

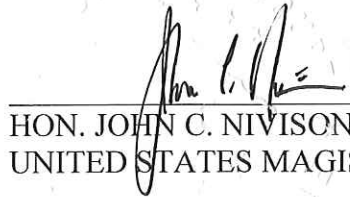
CONCLUSION

Based on the foregoing, there is probable cause to believe that the federal criminal statute cited herein has been violated, and that the property, evidence, and instrumentalities of this offense, more fully described in Attachment B, are to be found at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.



Michel J. Verhar
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 4th day of April, 2019



HON. JOHN C. NIVISON
UNITED STATES MAGISTRATE JUDGE